WILLKIE FARR & GALLAGHER LLP
BENEDICT Y. HUR (SBN: 224018)
bhur@willkie.com
SIMONA AGNOLUCCI (SBN: 246943)
sagnolucci@willkie.com
EDUARDO E. SANTACANA (SBN: 281668)
esantacana@willkie.com
LORI C. ARAKAKI (SBN: 315119)
larakaki@willkie.com
ARGEMIRA FLOREZ (SBN: 331153)
aflorez@willkie.com
HARRIS MATEEN (SBN: 335593)
hmateen@willkie.com
One Front Street, 34th Floor
San Francisco, CA 94111
Telephone: (415) 858-7400
Facsimile: (415) 858-7599

Attorneys for Defendant
GOOGLE LLC

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

ANIBAL RODRIGUEZ, et al. individually and on behalf of all others similarly situated,

Plaintiff,

vs.

GOOGLE LLC,

Defendant.

Case No. 3:20-CV-04688-RS

DECLARATION OF STEVE GANEM IN SUPPORT OF PLAINTIFFS' ADMINISTRATIVE MOTION TO SEAL (DKT. 272)

Judge:	Hon. Richard Seeborg
Courtroom:	3, 17th Floor
Action Filed:	07/14/2020
Trial Date:	Not Yet Set

I, STEVE GANEM, declare:

1. I am a Director of Product Management at Google LLC with supervisory authority concerning Google Analytics for Firebase ("GA for Firebase"). Unless otherwise stated, the facts I set forth in this declaration are based on my personal knowledge or knowledge I obtained through my review of corporate records or other investigation. If called to testify as a witness, I could and would testify competently to such facts under oath.

2. I submit this declaration in support of an Administrative Motion to Consider Whether Another Party's Material Should Be Sealed filed by Plaintiffs. Dkt. No 272. I have reviewed unredacted versions of Plaintiffs' Reply ISO Plaintiffs' Rule 15(a) Motion for Leave to Amend Complaint and Exhibits 34–39. *Id.*

3. Google seeks to seal narrowly tailored portions of only the following information, all of which I have reviewed.

Document	Portions Sought to Be Sealed
Reply (Dkt. 272-1)	Number of active Google Accounts with WAA or sWAA off; Project code name "Pr***Na***."
Exhibit 34 (Dkt. 272-2).	Number of active Google Accounts with WAA or sWAA off.
Exhibit 35 (Dkt. 272-3)	Project code name "Pr***Na***"; non-public email addresses of Google employees.
Exhibit 36 (Dkt. 272-4)	List of top Firebase customers; non-public email addresses of Google employees.
Exhibit 37 (Dkt. 272-5)	Google's response to Interrogatory No. 1.
Exhibit 38 (Dkt. 272-6)	Project code names "Na***" and "Do***."
Exhibit 39 (Dkt. 272-7)	Project code name "Pr***Na***"; non-public email addresses of Google employees.

4. Technical Details Concerning Google's Processing of Firebase Data. **Exhibit 37** discloses highly confidential and proprietary technical information concerning Google's

processing and storage GA for Firebase data. Exhibit 37 contains Google's fourth supplemental response to Interrogatory No. 1, and part of its third supplemental response, both of which I verified. Google's response to Interrogatory No. 1 contains the findings from an extensive fact investigation in which I participated to understand and confirm precisely how data flows through and is processed by Google. I understand that this interrogatory response was labeled "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY" by Google under the parties' stipulated Protective Order.

5. Because this declaration is being filed publicly, I will describe the technical, confidential information contained within Google's response to Interrogatory No. 1 at a high level of generality to avoid disclosing proprietary information.

6. Google's response to Interrogatory No. 1 reveals details about the flow of GA for Firebase data from app developer customers to and within Google in a way that discloses highly confidential, technical, and proprietary information. For example, at page 18, the interrogatory response includes a data-flow diagram that depicts data generation, bundling, consent checks, data flow, and storage decisions including logging and retention decisions. The response then describes each step in the back-end data flow process in detail. In sub-sections 1 and 2, both of which concern "Data Logging," the response identifies the fields Google has programmed its systems to log on both Android and iOS devices, including identifying by name the user identifiers and settings that are logged through GA for Firebase, as well as Firebase Cloud Messaging, Firebase Crashlytics SDK, and Firebase Remote Config SDK. *See* Ex. 37 at page 18–22. The response identifies how Google has designed the data flow system to bundle app measurement events to send to Google (*id*. at 20:10-17), and discusses how Google joins the app measurement data on the server side to other data (*id*. at 21:18-21). As another example, in sub-section 3, Google describes in detail the decisions it made in coding its GA for Firebase product to allow developers to send data to Google in bundled packets. Ex. 37 at pp. 22-23 ("Data Upload"). Google's response to Interrogatory No. 1 also discloses steps Google takes to conduct consent checks and what it does upon receiving the results of the checks, all of which is the

product of extensive internal research, analysis, and engineering. Ex. 37 at 23-25 ("Consent Checks and Technical Barriers to Joining").

7. This response also discloses Google's confidential and proprietary decisions concerning the design of its data logging system and "Encryption Technology." *See* Ex. 37 at 25-28. For example, Google discloses details about its "restricted need-based access process and audit procedure" for processing user data that is confidential. Next, Google's response discloses business decisions it has made concerning the GA for Firebase data it receives. Ex. 37 at 28-29. And the response discloses technical details concerning data processing steps and infrastructure. Ex. 37 at 30. In addition, this interrogatory response discloses a code name for a server ("G***") that receives user data. Ex. 37 at 24:20-23. As described below in Paragraph 16, there is a good reason to protect confidential names such as this one.

8. Google considers the information within its response to Interrogatory No. 1 which includes names, data fields, functionality, and infrastructure of its data storage, flow, and logging systems to be highly confidential and proprietary information. Revealing specifics about the backend functionality of Google's products, along with internal names of data fields and the structure of data processing and flow systems presents a serious risk of irreparable harm to Google. This information is competitively sensitive. If information such as data flow and infrastructure architecture is disclosed, competitors could infer how Google's products function, and how they are developed. Competitors could mimic Google's approach to data organization and storage to unfairly compete with Google's product offerings to Google's detriment.

9. Because this interrogatory response compiles in one place the flow of GA for Firebase data through Google in a way that is not typically compiled in a single document, it is particularly sensitive. A competitor could take this single interrogatory response and use it to understand the entire structure of Google's GA for Firebase system that has taken countless employee and engineer hours to develop, refine, and maintain.

10. Google carefully maintains the confidentiality of the proprietary information described in its response to Interrogatory No. 1 by limiting access to particular individuals and teams and storing it on secure servers. Google also keeps this information confidential in litigation.

11. Because the response to Interrogatory No. 1—in its entirety—discusses highly confidential, technical, and proprietary information concerning Google's data processing and storage systems and back-end data processing flow and infrastructure, the entire interrogatory response should be sealed. There is no way to adequately disentangle portions of the information that are highly confidential from others that are not. Google has tailored its request to allow the interrogatory requests and objections to be publicly filed, and no more limited sealing would appropriately protect Google's confidential information.

12. Confidential Business Information Concerning Google Account Product and Firebase Customer List. Plaintiffs' **Reply** and **Exhibits 34 and 36** disclose confidential business information that could harm Google's business if disclosed. Exhibit 34 is a set of Google's interrogatory responses. Google seeks to seal portions of its response to Interrogatory No. 12 that disclose the number of active Google accounts in the United States that have turned off the WAA and sWAA settings during an identified time period, at 5:18-20 and 6:3-4. Plaintiffs' Reply also discloses the same information, at 1:11. Exhibit 36 is a slide deck titled "Increase user engagement with Firebase & Google Analytics." Google seeks to seal part of one slide in the deck discloses by name and company logo a list of Google's top Firebase customers, at GOOG-RDGZ-00060729.

13. The number of active Google account holders who have the WAA and sWAA settings on or off comprises confidential business information. Competitors could use this information to target Google products that rely on those settings by understanding the volume of users who use those products. Similarly, Google's Firebase customer list and its identification of what it views as top customers is confidential and proprietary information that Google closely guards. Competitors who develop similar products for app developers could use the list to

specifically target those customers and induce them to switch from using Firebase to another product, which would unfairly harm Google's business.

14. This information should be shielded from unnecessary public disclosure. Google does not disclose it publicly in business dealings or in litigation. Google carefully maintains the confidentiality of the information it seeks to seal in Exhibits 34 and 36 by limiting access to particular individuals and teams within Google and maintaining the confidentiality of the information in litigation.

15. Google has narrowly tailored the information to be sealed. In Exhibit 34, Google's response to Interrogatory Number 12, Google only seeks to redact the numerical amount in the following two sentences: at 5:18-20 ("From July 27, 2016 to July 27, 2020, [REDACT] active Google Accounts in the United State turned off Web & App Activity settings…."), and at 6:3-4 ("From July 27, 2016 to July 27, 2020, [REDACT] active Google accounts in the United States turned off the "sWAA" setting …."). In the Reply, Google seeks to redact the numerical amount in the following sentence, at 1:10-12 ("Google has admitted that '[REDACT] active Google accounts in the United States turned off' either WAA or supplemental sWAA during the class period.'"). In Exhibit 36, Google only seeks to seal part of one slide in the deck that discloses by name and company logo a list of Google's top Firebase customers. Exhibit 36 at GOOG-RDGZ-00060729. No more narrowly tailored redactions would adequately protect Google's business interests in protecting its Google Account product and Firebase customer list.

16. References to Internal Project Names. Plaintiffs' **Reply** at 1:23, **Exhibit 35** at GOOG-RDGZ-00203545, and **Exhibit 38** at 6:23, 7:9, 11:17, and 102:17 all contain reference to an internal project name ("Pr***Na***"). **Exhibit 38** also references a different internal name ("Do***"). These documents also disclose details of those projects. Revealing Google's internal code names that correspond to descriptions of projects would present a serious risk of harm to Google. Specifically, an individual interested in improperly accessing Google's systems could target particular proprietary documents and information for improper uses if he or she knew Google's confidential internal names, Thus, it is very important that internal code names not be

revealed outside of Google. Google has narrowly tailored the information to be sealed to allow the first or second letter in each project name to be filed publicly, and no more limited sealing would appropriately protect Google's confidential and proprietary information.

17. Non-public Email Addresses. **Exhibits 35–36 and 39** contain confidential email addresses of Google employees. Google does not publish employee email addresses. Allowing these internal email addresses to become public presents a threat of harassment to the employees who may be contacted by members of the public. Specifically, an individual interested in contacting Google employees directly rather than following published channels for contacting Google may target those employees. Google has narrowly tailored the information to be sealed to allow the employee names and the Google domain name to be filed publicly. For example, when an email is sent from "First Name Last Name <uniqueaddress@google.com>," Google only proposes to seal the "uniqueaddress" part of the email. No more limited sealing would appropriately protect Google's confidential and proprietary information.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed November 28, 2022, at Irvine, California.

Steve Ganem